AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph that begins on line 18 of page 10 with the following amended paragraph:

Host 32 unseals (decrypts) the sealed transceiver 36 specific public key using the known corresponding public key of the issuing authority. Host 32 completes the authentication of transceiver 36 by generating a random number and passing the random <u>number</u> to security microcontroller 38. Security microcontroller 38 seals (encrypts) the random number using the transceiver 36 specific private key. In one embodiment, host 32 generates an authentication string in place of the random number for authentication. After security microcontroller 38 returns the result to host 32, host 32 uses the transceiver 36 specific public key obtained from the previously requested sealed transceiver 36 specific public key to decrypt the result. If the decrypted result matches the random number that host 32 generated, security microcontroller 38 contains the unique transceiver 36 specific private key associated with the transceiver 36 specific public key that was sealed by the issuing authority. Host 32 concludes that security microcontroller 38, and by extension transceiver 36 in which it is mounted, is authentic. If host 32 determines that transceiver 36 is authentic, host 32 accepts and uses transceiver 36. If, however, host 32 determines that transceiver 36 is not authentic, host 32 rejects and does not use transceiver 36.